REMARKS

In the Office Action dated March 7, 2005, claim 24 was objected to; claims 1, 5, 6, 8, 12-14, 22, 26, 27, 29, and 32-33 were rejected under 35 U.S.C. § 102 over U.S. Patent No. 6,185,185 (Bass); claims 16, 18, 19, 35, 37, 38, 42, 45-50, 52, and 54 were rejected under § 103 over Bass in view of U.S. Patent No. 6,393,465 (Leeds); claims 2, 9-11, 20, 23, 30, 31, and 39 were rejected under § 103 over Bass in view of U.S. Patent No. 6,578,086 (Regan); claims 3, 4, 24, 25, and 41 were rejected under § 103 over Bass in view of U.S. Patent No. 5,260,945 (Rodeheffer); claims 7, 15, 17, 28, 34, and 36 were rejected under § 103 over Bass in view of U.S. Patent No. 6,826,611 (Arndt); claims 21 and 40 were rejected under § 103 over Bass in view of Rodeheffer and U.S. Patent No. 6,453,430 (Singh); claim 43 was rejected under § 103 over Bass in view of Leeds and Regan; claim 44 was rejected under § 103 over Bass in view of Leeds, Singh, and Rodeheffer; claims 51, 55, and 56 were rejected under § 103 over Bass in view of Leeds and U.S. Patent No. 5,640,504 (Johnson); and claims 53, 57, and 58 were rejected under § 103 over Bass in view of Leeds and U.S. Patent No. 6,285,748 (Lewis).

Claim 41 has been cancelled, without prejudice, to render the rejection of the claim moot.

Claim 24 has been amended to address the objection raised with respect to the claim.

Amended claim 1 is not anticipated by Bass. Claim 1 now recites a method that includes, *inter alia*, monitoring the network for any patterns of behavior; determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior; and determining a proper action for mitigating that type of undesirable behavior, the proper action including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable behavior, where preventing dissemination comprises at least one of *changing a routing table, changing a forwarding table, turning off at least one port of a forwarding device, filtering on Internet Protocol (IP) addresses, and filtering on media access control (MAC) addresses*.

Bass describes a technique for reducing likelihood of broadcast storms in a network based on the transmission of multiple-destination messages (such as broadcast messages or multicast messages). Bass, 1:23-34; 2:11-14. Bass indicates that multi-destination messages are classified into multiple broadcast message classes, with a count associated with each broadcast

message class. Bass, 2:24-33. By distinguishing multiple-destination messages into different classes, different treatment can be provided for multi-destination messages of different classes. Bass, 2:37-44. If the count of a particular class of multiple-destination messages exceeds a threshold, then this class of multi-destination messages are discarded to reduce the likelihood of a broadcast storm. Bass, 6:6-10. However, Bass states that multi-destination messages of other classes (that do not have counts exceeding the threshold) can continue to be transmitted. Bass, 3:13-27.

Bass makes it clear that the action taken with respect to multi-destination messages of a class that exceeds a threshold is the *discarding* of these messages. Bass, 3:24-27; 7:41-48. There is no teaching whatsoever in Bass of preventing dissemination of packets associated with an undesirable behavior by any one of: (1) changing a routing table; (2) changing a forwarding table; (3) turning off at least one port of a forwarding device; (4) filtering on IP addresses; and (5) filtering on media access control addresses.

Since Bass does not disclose each and every element of claim 1, it is submitted that claim 1, and all its dependent claims, are allowable over Bass. The obviousness rejections of claims dependent from claim 1 have been overcome by the amendment of claim 1.

Amended independent claim 22 (and its dependent claims) are also allowable over Bass, which fails to disclose a means for determining a proper action for mitigating a type of undesirable behavior, where the proper action, performed by mitigation means, includes preventing dissemination through the network of packets associated with an undesirable behavior, and where preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, and turning off at least one port of a forwarding device.

The obviousness rejections of claims dependent from claim 22 have also been overcome by the amendment of claim 22.

It is respectfully submitted that independent claim 42 is not obvious over the asserted combination of Bass and Leeds. The Office Action conceded that Bass does not disclose the means for determining if the information about the pattern of behavior from any of the computers is trustworthy. 3/7/2005 Office Action at 6. Reliance was made on Leeds as teaching this missing element. It is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 42 for at least the following two reasons: (1) there existed

no motivation or suggestion to combine Bass and Leeds; and (2) even if combined, the hypothetical combination of Bass and Leeds does not disclose or suggest each and every element of the claim. *See* M.P.E.P. § 2143 (8th ed., Rev. 2), at 2100-129.

The second point above is addressed first. As conceded by the Office Action, Bass not disclose the means for determining if the information about the pattern of behavior from any of the computers is trustworthy. Moreover, contrary to the incorrect assertion in the Office Action, Bass also fails to disclose another element of claim 42, namely the means for monitoring the network for any patterns of behavior, including, if available, information about a pattern of behavior from *any of the computers about another one of the computers*. This monitoring means of claim 42 monitors information from one of the computers *about* another one of the computers. Monitoring for such information is not performed at all in Bass. In Bass, a switch 10 (see Fig. 1 of Bass) contains a mechanism that includes counters 13A-13C, 15A-15C, 17A-17C, for counting multiple-destination messages of different classes. Fig. 2 of Bass illustrates the operation of the switch 10. Bass, 6:34-35. The switch 10 increments the class count of a broadcast message. Bass, 7:13-27. Also, the switch 10 compares the class count of a broadcast message against a threshold to determine whether a packet is to be discarded or not. Bass, 7:28-49. What the switch 10 of Bass is monitoring is count information maintained by the counters *within* the switch 10. Thus, the information maintained by the counters cannot constitute information *from any of the computers about another one of the computers*.

Note that the network arrangement shown in Fig. 1 of Bass also depicts a computer 26 having a network interface 28 with counters 29A-29C. The network interface 28 can monitor counts of multiple-destination messages in a manner similar to that of switch 10 of Bass. A discussion of the operation of the network interface 28 in this regard is provided in Fig. 4 of Bass and the accompanying text. Again, the network interface 28 of Bass monitors counts maintained by counters 29A-29C in the network interface 28 for determining whether a transmitted or received packet at the computer 26 is to be discarded or not. Bass, 9:5-31. The counts maintained by the network interface 28 that are monitored by the mechanism in the network interface 28 for discarding packets do not constitute information *from any of the computers about another one of the computers*.

Therefore, the statement in the Office Action that Bass teaches the means for monitoring the network for any patterns of behavior, including, if available, information about a pattern of behavior from any of the computers about another one of the computers, is erroneous. The Office Action cited to column 3, lines 37-38, of Bass as teaching this element. That passage states: "In such an embodiment, network traffic is monitored so as to create class counts of messages for the plurality of broadcast message classes." The class count, as discussed above, is not information from one of the computers about another one of the computers. In view of this misapplication of Bass to one of the elements of claim 42, the obviousness rejection is defective since the hypothetical combination of Bass and Leeds does not teach or suggest all elements of claim 42.

The obviousness rejection is further defective for the reason that Leeds does not disclose or suggest the means for determining if the information about the pattern of behavior from any of the computers is trustworthy. Leeds describes a method and system for parsing and analyzing incoming electronic mail messages to determine a confidence factor indicative of whether or not messages are junk e-mail. Leeds, Abstract. Determining whether an incoming mail message is a junk e-mail, as performed by Leeds, is *not* the same as determining if information *about a pattern of behavior from any of the computers* is trustworthy. Leeds does not teach or even remotely suggest that the e-mails received by the authenticator of Leeds contains any information about a pattern of behavior. Thus, the citation of Leeds as teaching the means for determining if the information about the pattern of behavior from any of the computers is trustworthy is clearly erroneous, as Leeds does *not* teach or suggest the element conceded by the Office Action as missing from Bass. In view of the foregoing, it is respectfully submitted that the hypothetical combination of Bass and Leeds does not teach or suggest all elements of claim 42.

Moreover, there existed no motivation or suggestion to combine the teachings of Bass and Leeds. Bass relates to counting the number of multiple-destination messages of different classes to determine whether a threshold has been crossed to determine whether packets are to be discarded. On the other hand, Leeds describes an authenticator for determining whether incoming e-mail messages are junk e-mail. A person of ordinary skill in the art looking to the teachings of Bass and Leeds would not have been motivated to incorporate the authenticator of

Leeds into the system of Bass. There is absolutely no suggestion whatsoever in Bass of any desirability or need to incorporate an authenticator for detecting junk e-mail. The only motivation or suggestion to incorporate the teachings of Leeds into Bass is the teachings of the present disclosure. Thus, what the Office Action has performed is a classic example of using impermissible hindsight that involves piecing together completely un-related elements of prior art references to achieve the claimed invention, where no teaching or suggestion existed to make such combination.

The obviousness rejection is defective for this further reason. In view of the foregoing, it is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 42.

Claims dependent from claim 42 are allowable for at least the same reasons. In view of the defective application of Bass and Leeds to claim 42, the obviousness rejections of claims dependent from claim 42 over Bass and Leeds, or over Bass and Leeds and other references, have also been overcome.

Newly added independent claim 59 recites a method that comprises monitoring a network for an undesirable pattern comprising at least one of a stolen Internet Protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many probe packets directed to a firewall, and too many address resolution protocol (ARP) packets. The method of claim 59 also includes determining a type of the undesirable pattern, and determining an action to mitigate the undesirable pattern based on the type of undesirable pattern, where the action comprises preventing dissemination over the network of packets associated with the undesirable pattern.

Bass teaches detecting for broadcast storms – Bass does not teach detecting for stolen IP address, stolen MAC address, a malformed packet, too many probe packets directed to a firewall, and too many ARP packets. Therefore, claim 59 is not anticipated by Bass.

The subject matter of claim 59 incorporates part of the subject matter of claim 7 (which depends from claim 1). The Office Action had rejected claim 7 over the asserted combination of Bass and Arndt. 3/7/2005 Office Action at 14. The Office Action conceded that Bass does not teach that the undesirable pattern includes at least one of a stolen IP address, a stolen MAC address, a malformed packet, too many probe packets directed to a firewall, and too many ARP

packets. 3/7/2005 Office Action at 15. However, the Office Action relied upon Arndt as teaching this feature, citing specifically to column 1, lines 15-25, of Arndt. Arndt, in the cited passage, refers to difficulty in identifying correct local address ranges due to an incorrect subnet mask and mis-configured IP addresses. There is no mention here of monitoring for a *stolen* IP address, or any of the other elements of claim 59. Therefore, even if Bass can be combined with Arndt, the asserted combination of Bass and Arndt does not teach or suggest all elements of claim 59. Therefore, a *prima facie* case of obviousness cannot be established with respect to claim 59 over the asserted combination of Bass and Arndt.

Newly added independent claim 61 recites a system having a network interface to a network, and a packet traffic monitor to: monitor the network for an undesirable behavior; determine a type of the undesirable behavior; *discover a topology of the network*; and cause prevention of dissemination over the network of packets associated with the undesirable behavior based on the type of the undesirable behavior and *topology of the network*.

Bass does not disclose discovering a topology of the network and causing prevention of dissemination over the network of packets associated with the undesirable behavior based on the topology of the network. This point was conceded by the Office Action. *See* 3/7/2005 Office Action at 10.

However, the Office Action argued that a secondary reference, Regan, teaches the discovering of a topology of the network. 3/7/2005 Office Action at 11. Applicant respectfully submits that the hypothetical combination of Bass and Regan does not teach or suggest all elements of claim 61. Therefore, a *prima facie* case of obviousness cannot be established with respect to claim 61 over the asserted combination of Bass and Regan.

Regan describes use of a Spanning Tree Protocol (STP) that is designed to allow bridges to map a network for topology while eliminating loops which could lead to broadcast storms. Regan, 2:7-13. Regan also teaches a bridge that employs a prior distance vector protocol and learning processes to manage the topology of a bridge network layer. Regan, 4:56-59. Additionally, the network topology information is retained in a filtering database that is configured by a management action or by a learning process and algorithm. Regan, 6:40-45. There is no teaching in Regan of discovering a topology of the network, *in combination with* causing prevention of dissemination over the network of packets associated with the undesirable

behavior based *on the topology of the network* (as well as based on the type of the undesirable behavior). Thus, the hypothetical combination of Bass and Regan does not teach or suggest all elements of claim 61.

Newly added dependent claims 60, 62, and 63 are allowable for at least the same reasons as corresponding independent claims.

Allowance of all claims is respectfully requested. The Commissioner is authorized to charge any additional fees and/or credit any overpayment to Deposit Account No. 08-2025 (200301735-2).

Respectfully submitted,

Date: June 7, 2005

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Suite 100
Houston, TX 77024
Telephone: (713) 468-8880
Facsimile: (713) 468-8883